RFC-0015 Recommended Secure Configuration Standard

RFC Front Matter

- **Status:** Open
- **Created By:** FedRAMP
- **Start Date:** 2025-09-10
- **Closing Date:** 2025-10-10
- **Short Name:** rfc-0015-recommended-secure-configuration

Where to Comment

Members of the public may submit multiple different comments on different issues during the public comment period. The public is asked to please refrain from including documents or spåreadsheets (especially those with in-line comments or suggested changes) in public comment as this creates a significant additional review burden.

Formal public comment for official consideration by FedRAMP can be made via the following mechanisms in order of preference:

1. GitHub Post: https://github.com/FedRAMP/community/discussions/84
2. Public Comment Form: https://forms.gle/gx9UbFAgZMYikkGt7
3. Email: pete@fedramp.gov with the subject "**RFC-0015 Feedback**"

Note: FedRAMP will review and publicly post all public comments received via email, but will not otherwise respond. Email submissions from federal agencies will only be made public when requested by the agency.

Summary & Motivation

This standard is required by Executive Order 14144, as amended by Executive Order 14306.

Cloud service providers nearly always provide guidance to customers with recommended secure configurations for critical services. This standard formalizes requirements and recommendations from FedRAMP about specific recommendations on secure configurations that agency customers should have in advance while setting up a cloud service offering.

This standard will apply to both FedRAMP 20x and FedRAMP Rev5 when formalized, without beta testing for Rev5. FedRAMP anticipates coordinating with all necessary parties to improve this standard over time.

Effective Date(s) & Overall Applicability

This is a draft standard released for public comment; it does not apply to any FedRAMP authorization and MUST NOT be used in draft form.

- FedRAMP **20x**:
    - This standard will apply to all FedRAMP 20x authorizations when formalized, including Phase Two pilot authorizations.
- FedRAMP **Rev5**:
    - This standard will apply to all FedRAMP Rev5 authorizations when formalized; it may remain optional or be required, pending determination by the FedRAMP Board.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.

- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Background & Authority

Executive Order 14144 “Strengthening and Promoting Innovation in the Nation’s Cybersecurity” Section 3 (d), as amended by Executive Order 14306 “Sustaining Select Efforts to Strengthen the Nation’s Cybersecurity and Amending Executive Order 13694 and Executive Order 14144” to Section 3 (b), states “*the Administrator of General Services, acting through the Director of the Federal Risk and Authorization Management Program (FedRAMP), in coordination with the Secretary of Commerce, acting through the Director of NIST, and the Secretary of Homeland Security, acting through the Director of CISA, shall develop FedRAMP policies and practices to incentivize or require cloud service providers in the FedRAMP Marketplace to produce baselines with specifications and recommendations for agency configuration of agency cloud-based systems in order to secure Federal data based on agency requirements.*”

Purpose

FedRAMP’s existing “System Security Plan Appendix J: CSO CIS and CRM Workbook” meets the requirements outlined in this executive order but does not effectively support the underlying intent: all customers benefit from simple, easy to follow, easy to understand instructions for securely configuring a cloud service offering. Cloud service providers often provide a wide range of configuration options to allow individual customers to pick and choose their security posture based on their individual customer needs and are best positioned to provide instructions about the overall security impacts of many of these choices.

This standard outlines simple requirements for FedRAMP authorized cloud service providers to effectively communicate the security impact of common settings to new and current federal agency customers.

Definitions

FRD-RSC-01

Top-level administrative account: The most privileged account with the highest level of access within a *cloud service offering* for a customer organization, typically with complete control over all aspects of the *cloud service offering*, including managing resources, users, access, privileges, and the account itself.

NOTE: Any references to *top-level administrative accounts* in FedRAMP materials should be presumed to apply to top-level administrative roles or other similar capabilities that are used to assign *top-level administrative account* privileges.

FRD-RSC-02

Privileged account: An account with elevated privileges that enables administrative functions over some aspect of the *cloud service offering* that may affect the confidentiality, integrity, or availability of information beyond those given to normal users; levels of privilege may vary wildly.

NOTE: Any references to *privileged accounts* in FedRAMP materials should be presumed to apply to privileged roles or other similar capabilities that are used to assign privileges to *privileged accounts.*

Requirements

FRR-RSC

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-RSC-01

Providers MUST create and maintain guidance that includes instructions on how to securely access, configure, operate, and decommission *top-level administrative accounts* that control enterprise access to the entire *cloud service offering*.

NOTE: This guidance should explain how *top-level administrative accounts* are named and referred to in the *cloud service offering.*

FRR-RSC-02

Providers MUST create and maintain guidance that explains all settings that can be operated only by *top-level administrative accounts* and their security implications.

FRR-RSC-03

Providers SHOULD create and maintain guidance that explains all settings that can be operated only by other *privileged accounts* and their security implications.

FRR-RSC-04

Providers SHOULD set all settings to their recommended secure defaults for *top-level administrative accounts* and *privileged accounts* when initially provisioned.

FRR-RSC-05

Providers SHOULD offer the capability to compare all current settings for *top-level administrative accounts* and *privileged accounts* to the recommended secure defaults.

FRR-RSC-06

Providers SHOULD offer the capability to export all security settings in a machine-readable format.

FRR-RSC-07

Providers SHOULD offer the capability to view and adjust security settings via an API or similar capability.

FRR-RSC-08

Providers SHOULD provide recommended secure configuration guidance in a *machine-readable* format that can be used by customers or third-party tools to compare against current settings.

FRR-RSC-09

Providers SHOULD make recommended secure configuration guidance available publicly.

FRR-RSC-10

Providers SHOULD provide versioning and a release history for recommended secure default settings for *top-level administrative accounts* and *privileged accounts* as they are adjusted over time.